

IN THE CLAIMS:

Please amend claims 1-3 and 36-38 as indicated below.

A listing of the status of all claims 1-38 in the present patent application is provided below.

1 (Currently Amended). A method for providing computer security, comprising:

determining, using a processor, whether an executable associated with a static state meets [a] one or more first predetermined ~~exiterion~~ criteria;

associating a first risk level with the executable, ~~if it is determined that~~ based upon whether the executable meets the one or more first predetermined ~~exiterion~~ criteria;

determining whether ~~observing that~~ a current process ~~started by~~ associated with the executable meets one or more second predetermined criteria ~~has performed or has attempted to perform an action with which a second risk level, being a higher level than the first, is associated~~;

associating ~~updating the first risk level to the~~ a second risk level with the current process ~~based on the observation upon whether the current process meets the one or more second predetermined criteria, wherein the current process is initially associated with the first risk level, and wherein the first risk~~

level is updated to the second risk level for the current process based upon whether the current process meets the one or more second predetermined criteria; and

performing a predetermined responsive action with respect to the process if the second risk level exceeds ~~the~~ a threat detection threshold;

wherein determining whether the executable meets the one or more first predetermined ~~criterion~~ criteria does not comprise comparing ~~compare~~ the executable with a virus signature.

2 (Currently Amended). The method for providing computer security as recited in Claim 1, wherein the first risk level indicates a level of potential risk that will be brought by operating the executable.

3 (Currently Amended). The method for providing computer security as recited in Claim 1, wherein the first risk level indicates how much risk the executable presents.

4 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a configuration criterion.

5 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured as a service.

6 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured to run under a highly privileged account.

7 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is installed via a standard procedure.

8 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has sufficient access control.

9 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is

modified.

10 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is signed.

11 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has a modified date different from created date.

12 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a capability criterion.

13 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has networking capability.

14 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has

privilege manipulation capability.

15 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has remote process capability.

16 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has process launching capability.

17 (Previously Presented). The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has secure coding violation.

18 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising associating with the executable a risk type indicating a type of risk to which the executable is vulnerable.

19-28 (Cancelled).

29 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence.

30 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a record of activities.

31 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a log file.

32 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a system optimization file.

33 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a

crash dump file.

34 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a prefetch file.

35 (Previously Presented). The method for providing computer security as recited in Claim 1, further comprising performing a dynamic risk analysis.

36 (Currently Amended). The method for providing computer security as recited in Claim 1, further comprising determining whether ~~[an]~~ the predetermined responsive action is required.

37 (Currently Amended). A system for providing computer security, comprising:

a processor configured to:

determine whether an executable associated with a static state meets [a] one or more first predetermined ~~criterion~~ criteria;

associate a first risk level with the executable ~~criterion, if it is determined that~~ based upon whether the

executable meets the one or more first predetermined ~~riterion~~
criteria;

determine whether ~~observe that~~ a current process
~~started by~~ associated with the executable meets one or more
second predetermined criteria ~~has performed or attempted to~~
~~perform an action with which a second risk level, being a higher~~
~~level than the first, is associated;~~

associate ~~update the first risk level to the~~ a second
risk level with the current process based ~~on the observation~~
upon whether the current process meets the one or more second
predetermined criteria, wherein the current process is initially
associated with the first risk level, and wherein the first risk
level is updated to the second risk level for the current
process based upon whether the current process meets the one or
more second predetermined criteria; and

perform a predetermined responsive action with respect
to the process if the second risk level exceeds the a threat
detection threshold;

wherein determining whether the executable meets [a]
the one or more first predetermined ~~riterion~~ criteria does not
comprise comparing ~~compare~~ the executable with a virus
signature; and

a memory, coupled with the processor, configured to provide

the processor with instructions.

38 (Currently Amended). A computer program product for providing computer security, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

determining whether an executable associated with a static state meets [a] one or more first predetermined criterion criteria;

associating a first risk level with the executable ~~criterion, if it is determined that based upon whether the~~ executable meets the one or more first predetermined criterion criteria;

~~determining whether observing that a current process started by~~ associated with the executable meets one or more second predetermined criteria ~~has performed or has attempted to perform an action with which a second risk level, being a higher level than the first, is associated;~~

~~associating updating the first risk level to the a~~ second risk level with the current process based on the observation upon whether the current process meets the one or more second predetermined criteria, wherein the current process is initially associated with the first risk level, and wherein the first risk

level is updated to the second risk level for the current process based upon whether the current process meets the one or more second predetermined criteria; and

performing a predetermined responsive action with respect to the process if the second risk level exceeds ~~the~~ a threat detection threshold;

wherein determining whether the executable meets [a] the one or more first predetermined ~~criteria~~ criteria does not comprise comparing ~~compare~~ the executable with a virus signature.